

NEWS

United States Department of Justice
U.S. Attorney, District of New Jersey
970 Broad Street, Seventh Floor
Newark, New Jersey 07102



Christopher J. Christie, U.S. Attorney

More Information? Call the Assistant U.S. Attorney or other contact listed below to see if more information is available.

News on the Internet: News Releases and related documents are posted at our website, along with links to our archived releases for other years. ***Go to:*** www.usdoj.gov/usao/nj/press/

Assistant U.S. Attorneys:
EREZ LIEBERMANN
and MARC FERZAN
973-645-2874 and 2783, respectively

lin1219.rel
FOR IMMEDIATE RELEASE
Dec. 19, 2006

Systems Administrator Arrested on Indictment Charging
Him with Setting Computer “Logic Bomb” at Public Company

(More)

Public Affairs Office
Michael Drewniak, PAO

973-645-2888

Breaking News: <http://www.usdoj.gov/usao/nj/publicaffairs>

NEWARK – A computer systems administrator for Medco Health Solutions, Inc. was charged today with allegedly planting a “logic bomb” in Medco’s computer systems. The logic bomb planted by the defendant would have caused widespread financial damages and potential health risks to Medco customers, U.S. Attorney Christopher J. Christie announced.

Yung-Hsun Lin a/k/a “Andy Lin,” 50, of Montville, New Jersey, was arrested at his home this morning by Special Agents of the FBI, on a two-count Indictment returned under seal yesterday by a federal grand jury. The Indictment alleges that Lin planted the logic bomb in Medco’s HP-Unix servers and would have wiped out critical data stored on more than 70 servers, according to Assistant U.S. Attorney Erez Lieberman.

Lin, who worked in Medco’s Fair Lawn offices, is scheduled to make an initial appearance at 2:30 p.m. today before U.S. Magistrate Judge Mark Falk. The case has been assigned to U.S. District Judge Jose L. Linares before whom Lin is scheduled to be arraigned on the Indictment on Jan. 3.

Among the databases operated from the affected servers was a critical one maintained and updated regularly by Medco – a patient-specific drug interaction conflict database known as the Drug Utilization Review (DUR). Prior to dispensing medication, pharmacists routinely examined the information contained in the DUR to determine whether conflicts existed between or among an individual's prescribed drugs.

In addition to the DUR, the servers contained applications relating to clients' clinical analyses, rebate applications, billing, and managed care processing. Further, the servers handled new prescription call-ins from doctors and coverage determination applications, as well as numerous internal Medco applications, including the corporate financials, pharmacy maintenance tracking, web and pharmacy statistics reporting, and the employee payroll input.

The logic bomb initially failed to “detonate” on the intended day, was allegedly modified by the defendant to execute again, but was then detected by the company and neutralized.

“The potential damage to Medco and the patients and physicians served by the company cannot be understated,” said Christie. “A malicious program like this can bring a company’s operations to a grinding halt and cause millions of dollars in damage from lost data, system downtime, recovery and repair.”

“Companies and law enforcement must be extremely vigilant to guard against disgruntled employees with the knowledge and position to wreak such havoc,” Christie added.

Christie credited Medco for it’s detection of the program before the damage could unfold.

This is the second recent prosecution, and the third in five years, by the U.S. Attorney's Office for the District of New Jersey of a systems administrator accused of planting a logic bomb in a corporate computer network. Last week, former UBS Paine Webber systems administrator Roger Duronio, 63, of Bogota, N.J., was sentenced to 97 months in prison for setting a logic bomb that did considerable damage to UBS computers. Duronio went to trial and was convicted. A third prosecution of a systems administrator at a private New Jersey high-tech company also ended in conviction. That defendant, Allen Lloyd of Wilmington, Del., received a 41-month prison sentence in 2002.

Lin is charged with two counts of fraud related to activity in connection with computers – one count for exceeding authorized access with intent to cause damage in excess of \$5,000; the other for the impairment, or potential impairment, of the medical examination, diagnosis, treatment or medical care of one or more individuals. Each count carries a maximum statutory penalty of 10 years in prison and a \$250,000 fine.

According to the Indictment, when Medco, based in Franklin Lakes, spun off from Merck & Co. in 2003, Lin feared that layoffs may affect him. In September 2003, e-mails were circulated among Lin and others discussing the anticipated layoffs of Medco computer system administrators. Then, on Oct. 3, 2003, Lin created the logic bomb by modifying existing computer code and inserting new code into Medco's servers. Part of the new computer code Lin allegedly programmed and inserted included a script designed to deploy the logic bomb automatically on April 23, 2004 – Lin's birthday.

Even after retaining his employment following the Oct. 6, 2003 layoffs, Lin did not remove the logic bomb from the Medco servers. Instead, Lin tweaked the destructive code in November 2003. Due to an error in the logic bomb, however, it failed to cause damage on April 23, 2004.

Lin kept the logic bomb in place after it failed to deploy, and, according to the Indictment, between September 20, 2004 and September 22, 2004, Lin modified the logic bomb to correct the error which prevented the code from executing as planned. After the correction, the logic bomb was set to deploy on April 23, 2005.

On Jan. 1, 2005, a Medco computer systems administrator investigating a system error discovered the logic bomb embedded within other scripts on Medco's servers. Medco information technology security personnel subsequently neutralized the destructive code.

Despite Indictment, every defendant is presumed innocent, unless and until found guilty beyond a reasonable doubt.

Christie credited the Special Agents of the FBI, under the direction of Special Agent in

Charge Leslie G. Wiser, Jr., with the investigation leading to Lin's arrest.

The case is being prosecuted by Assistant U.S. Attorney Erez Liebermann of the U.S. Attorney's Computer Hacking and Intellectual Property Section, and Marc Ferzan, Chief of the U.S. Attorney's Commercial Crimes Unit in Newark, New Jersey.

-end-

Defense Counsel: Raymond Wong, Esq., New York.